IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend LILIANA T. HANLON, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	Case No. 1:21-cv-04976
v.	)	
	)	Hon. Martha M. Pacold
SAMSUNG ELECTRONICS AMERICA, INC.,	)	
Defendant.	)	

AMENDED CLASS ACTION COMPLAINT

Plaintiff G.T., a minor by and through next friend Liliana T. Hanlon, individually and on behalf of all other persons similarly situated, brings this class action lawsuit for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*., against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"). Plaintiff alleges the following facts based on personal knowledge, investigation by counsel, and on information and belief where indicated.

NATURE OF THE ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Samsung in collecting, storing, and using their and other similarly-situated individuals' biometric identifiers[1] and biometric information[2] (collectively,

[1] A "biometric identifier" is any personal feature that is biologically unique to an individual, such as retina scans, fingerprints, and scans of face geometry. 740 ILCS 14/10.

[2] "Biometric information" is any information based on a person's biometric identifier used to identify an individual. 740 ILCS 14/10.

"Biometrics") without obtaining informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers" such as social security numbers, which can be changed if compromised. 740 ILCS 14/5(c). "Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. Recognizing the need to protect citizens from these risks, Illinois enacted BIPA, which prohibits private entities like Samsung from collecting, capturing, obtaining and/or possessing an individual's Biometrics unless they first: (1) inform that person in writing that biometric identifiers or information will be collected or stored; (2) provide that person with written notice of the specific purpose and length of term for which such biometric identifiers and/or information is being collected, stored, and used; (3) receives a signed written release from the person authorizing the collection of his or her biometric identifiers and/or information; and (4) develops and complies with a publicly-available retention schedule and guidelines for permanently destroying biometric identifiers and/or information. *See* 740 ILCS 14/15(a)-(b).

4. In direct violation of these requirements, Samsung collected, captured, stored and used—without first providing notice, obtaining informed written consent, or publishing data retention and destruction policies—the Biometrics of millions of unwitting Illinois residents whose faces appear in photographs stored on Samsung mobile devices ("Samsung Devices") in Illinois.

5. Through its Gallery software application ("Gallery App"), Samsung created, captured, collected, and stored millions of unique "face templates" (*i.e.* highly detailed geographic maps of facial features) from the photos stored on Samsung Devices—including photos of users,

non-users, and even minors. Much like fingerprints, voiceprints, and retinal patterns, each face template is unique to, and can be used to identify, a particular person.

6. Samsung's Gallery App, which comes pre-installed on Samsung Devices and cannot removed or modified, creates these face templates using sophisticated facial recognition technology that analyzes and extracts the points and contours of faces that appear in the photos stored on Samsung Devices. All of this occurs automatically through a "background" process in the Gallery App, without the knowledge or informed written consent of the user, let alone anyone else who appears in the photographs stored on Samsung Devices.

7. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of Illinois residents, and to recover statutory damages for Defendant's unauthorized collection, storage and use of these individuals' Biometrics in violation of BIPA.

PARTIES

8. Plaintiff G.T., a minor, is and has been at all times relevant a resident of Champaign in Champaign County, Illinois.

9. Liliana T. Hanlon, G.T.'s next friend, is and has been at all times relevant a resident of Champaign in Champaign County, Illinois.

10. Defendant Samsung Electronics America, Inc., the designer, manufacturer, and vendor of Samsung smartphones, tablets, and apps, is a corporation organized under New York law. Defendant Samsung regularly conducts business in this County and throughout the State of Illinois.

JURISDICTION AND VENUE

11. This Court has jurisdiction over Samsung pursuant to 735 ILCS 5/2-209 based on the commission of a tortious act in Illinois.

12. Venue is proper under 735 ILCS 5/1-101 and 735 ILCS 5/2-102(a) because Samsung regularly conducts business in this County, and maintains its principle place of business in this County.

FACTUAL BACKGROUND

I. Illinois's Biometric Information Privacy Act.

13. Biometrics are unlike other identifiers because they are a permanent, biologically-unique identifier associated with the individual. Because one cannot simply change her fingerprints or facial geometry, the collection, use, and storage of biometric identifiers and biometric information creates a heightened risk of identity theft. *See* 740 ILCS 14/5(c).

14. In the 2000's, major national corporations started using Chicago and other locations in Illinois to test new applications of biometric-facilitated transactions. *See* 740 ILCS 14/5(b).

15. In late 2007, a biometric company called Pay by Touch—which provided major retailers throughout the State of Illinois with biometric scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois legislature because suddenly there was a serious risk that citizens' biometric records—which can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections. The bankruptcy also highlighted that many persons who used the biometric scanners were unaware that the scanners were transmitting their data to the now-bankrupt company, and that their biometric identifiers could then be sold to unknown third parties.

16. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276.

17. BIPA makes it unlawful for a company to collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information unless the company first:

a) informs the subject in writing that a biometric identifier or information is being collected or stored;

b) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or information is being collected, stored, and used; and

c) receives a written release executed by the subject of the biometric identifier or information.

740 ILCS 14/15(b).

18. BIPA defines a "written release" as "informed written consent." 740 ILCS 14/10.

19. BIPA also requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting such identifiers or information has been satisfied, or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

20. One of the most prevalent uses of biometric identifiers is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific details about the face's geometry as determined by facial points and contours, and comparing the resulting "face template" (or "faceprint") to the face templates stored in a face template database. If a database match is found, an individual may be identified.

21. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and

carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

22. As alleged below, Samsung's practice of collecting, storing and using individuals' biometric identifiers (specifically, their facial geometry) and associated biometric information without informed written consent violated all three prongs of BIPA § 15(b). Samsung's failure to develop a publicly-available written policy regarding its retention schedule and guidelines for the permanent destruction of individuals' biometric identifiers and biometric information, and Samsung's failure to permanently destroy the biometric identifiers and biometric information, violated BIPA § 15(a).

II. Samsung Collected Plaintiff's Biometrics.

23. Samsung's facial recognition technology is offered as a "feature" of its Gallery App that is included by default in its operating systems and pre-installed on Samsung Devices sold to consumers.

24. The facial recognition "feature" of Samsung's Gallery App uses an algorithm that scans a user's photo library for faces, and then calculates a unique digital representation of each face (*i.e.* the face template) based on geometric attributes such as distance between the eyes, the width of the nose, and other features. Accordingly, these face templates each constitute a "biometric identifier." *See* 740 ILCS 14/10.

---

[3] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.judiciary.senate.gov/download/statement-of-franken-pdf (last visited Feb. 7, 2020).

[4] *Id.*

25. Samsung stores the face templates extracted from the user's photo library in a facial recognition database, or facial database, in the solid state memory on the user's Samsung Device.

26. The Gallery App uses these face templates to organize and sort photos based upon the particular individuals who appear in the photos. This is accomplished by comparing the face templates of individuals who appear in newly-stored photos against those already saved in the facial database. If there is a match, the Gallery App groups the newly-uploaded photo with previously-stored photos depicting the same individual.

27. Through its Gallery App, Samsung creates a unique face template for every face detected in the photographs stored on the user's Samsung Device. This is an automated process that occurs without the user's involvement or consent whenever a new photograph is stored on a Samsung Device.

28. Users cannot disable this facial recognition technology, nor can they prevent Samsung from harvesting the biometric identifiers (*i.e.* scans of face geometry) from the photographs stored on their Samsung Devices. Samsung provides no mechanism by which anyone may opt out of this process.

29. Consumers who buy Samsung Devices own the hardware, but merely license the software necessary for the device to function. That software is wholly owned and controlled by Samsung, as confirmed by Samsung's End User License Agreements ("EULAs"). The EULAs provide, in pertinent part:

> Samsung grants you a limited non-exclusive license to install, use, access, display and run one copy of the Samsung Software on a single Samsung Mobile Device[.] *** Samsung reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright and other intellectual property laws and treaties. Samsung or its suppliers own the title, copyright and other intellectual property rights in the Samsung Software. The Samsung Software is licensed, not sold.

30. Under the terms of the EULAs, the Samsung Device user is prohibited from modifying or altering the software.

31. Because disabling facial recognition is not permitted by Samsung, the use of Samsung Devices to take or store photographs is *conditioned* on the collection of Biometrics.

32. Samsung indiscriminately collects Biometrics for all photographic subjects, including customers, non-customers, and minors incapable of providing informed consent.

33. Samsung's Privacy Policy, in a supplement for California residents, confirms that "biometric information" is among the types of personal information Samsung collects.[5]

III. Samsung Possesses Plaintiff's Biometrics.

34. Although, on information and belief, Samsung does not store or transfer all user Biometrics on or by means of its servers, it has complete and exclusive control over the Biometrics collected and stored on Samsung Devices. To be clear, Samsung controls:

- Whether biometric identifiers are collected;
- What biometric identifiers are collected;
- The type of Biometrics that are collected and the format in which they are stored;
- The facial recognition algorithm that is used to collect Biometrics;
- What Biometrics are saved;
- Whether information based on biometric identifiers is used to identify users (thus creating biometric information);
- Whether Biometrics are kept locally on users' Samsung Devices;
- Whether Biometrics are encrypted or otherwise protected; and
- How long Biometrics are stored.

[5] *See* Samsung Privacy Policy for the U.S., *available at* https://www.samsung.com/us/account/privacy-policy/ (last visited August 4, 2021).

35. The user of a Samsung Device, in contrast, has no ability to control the Biometrics on the user's Samsung Device.

36. The user has no control over whether Biometrics are collected from the user's photo library.

37. Users cannot disable the collection of Biometrics or limit what information is collected or from whom it is collected. Indeed, Samsung's EULAs specifically *prohibit* users from modifying Samsung's software to prevent the collection of Biometrics.

38. Thus, Samsung fully controls—and thus possesses—the Biometrics on Samsung Devices.

IV. Samsung's Conduct Violates BIPA.

39. In violation of BIPA § 15(a), Samsung does not have a written, publicly-available policy establishing a retention schedule or guidelines for permanently destroying the biometric identifiers and biometric information it collected or otherwise obtained, and Samsung did not permanently destroy those within the statutorily-mandated timeframes.

40. In violation of BIPA § 15(b)(1), Samsung collected or otherwise obtained Illinois residents' biometric identifiers and biometric information without first informing them in writing that their biometric identifiers and biometric information were being collected or stored.

41. In violation of BIPA §§ 15(b)(2) and 15(b)(3), Samsung collected or otherwise obtained Illinois residents' biometric identifiers and biometric information without first informing them in writing of the specific purpose and length of time for which their biometric identifiers and information would be collected, stored and used, and obtaining a written release executed by each of those individuals.

42. Defendant's failure to comply with BIPA extends to nonusers of its devices. This is because Defendant's Gallery App collects and possesses the Biometric Data of *everyone* who appears in images stored in a Samsung Device user's photo library.

43. Samsung developed the facial recognition feature of its Gallery App, in part, to compete with other electronic device vendors and software developers, and in order to sell Samsung Devices.

V. Samsung's BIPA Violations Expose Plaintiff and the Other Class Members to Threats of Serious Harm.

44. Samsung does not delete the Biometrics it collects, which are located on numerous devices in this State.

45. A Samsung Device user's Biometrics may be stored on one or more Samsung Devices in use, as well as on discarded Samsung Devices.

46. Furthermore, non-users' Biometrics that Samsung collects may be stored on one or more Samsung Devices as well as on discarded Samsung Devices.

47. For example, an Illinois resident's Biometrics may be stored on his or her own Samsung Device(s) and/or on the Samsung Devices of his or her family members, relatives, friends, coworkers, and anyone else who photographed him or her using a Samsung Device or stored a photograph of him or her on a Samsung Device.

48. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach. By contrast, as the result of the fact that the Biometrics Samsung collects are stored on numerous devices, Plaintiff and members of the Class face the imminent threat of disclosure of their Biometrics as a result of a data breach on any one of the Samsung Devices on which their Biometrics are stored.

49. Samsung has nearly a 30% market share of the smartphone market in the United States,[6] and a 17.6% marketshare of the tablet market.[7] 85% of adult Americans use smartphones, and 53% use tablets.[8]

50. Many of the Samsung Devices used in this State have collected the Biometrics of multiple individuals other than the Samsung Device user. Consequently, numerous Illinois residents have their Biometrics stored on one or more Samsung Devices outside their control.

51. The durability of the memory in Samsung Devices creates a near-permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose Biometrics have been collected. Samsung Devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields.[9] Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the Biometrics on Samsung Devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

52. Biometrics may persist on discarded Samsung Devices, which could be extracted by malicious actors using methods of removal that may or may not currently exist.[10] The risk of

---

[6] Chance Miller, *Canalys: Apple Shipped 14.6M iPhones in North America During Ql, Securing 40% Marketshare*, 9to5Mac (May 9, 2019 3:23 PM), https://9to5mac.com/2019/05/09/iphone-north-america-marketshare/.

[7] Tablet Vendor Market Share United States of America (June 2021), *available at* https://gs.statcounter.com/vendor-market-share/tablet/united-states-of-america.

[8] *Mobile Fact Sheet*, Pew Research Center (Apr. 7, 2021), *available at* https://www.pewresearch.org/internet/fact-sheet/mobile/.

[9] Roderick Bauer, *SSD 101: How Reliable are SSDs?*, BackBlaze (Feb. 21, 2019), https://www.backblaze.com/blog/how-reliable-are-ssds/.

[10] *See, e.g.*, Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), https://www.rapid7.com/blog/post/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/; Federal Trade Commission, *How to Protect Your Phone and the Data On It*, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it (last

illicit harvesting of Biometrics from discarded Samsung Devices therefore extends far into the future.

VI. Samsung Is Directly and Vicariously Liable for Its BIPA Violations.

53. Samsung is directly liable for the BIPA violations based on the functionality of its proprietary software, which it wholly owns and exclusively controls, and which Samsung Device users are prohibited from owning, controlling, or modifying.

54. Furthermore, Samsung is vicariously liable for BIPA violations because its software operated as a "software agent":

> A software agent is essentially a software version of a concept familiar in the law: an entity that performs a task, with some degree of autonomy, on behalf of someone else. An agent in the physical world can perform its task without input from the principal; this is equally true when an agent is a machine, such as a robot on a factory floor, which can perform its repetitive task without needing constant human guidance. A software agent operates in the same way—it can perform its task without human input. For example, a software agent useful to shoppers could scan a large number of websites for a certain product, and identify the website offering the product at the lowest price; without such a program, the human user would have to look at each website herself.

NetFuel, Inc. v. F5 Networks, Inc., No. 13 C 7895, 2017 U.S. Dist. LEXIS 101587, at *3-4 (N.D. Ill. June 29, 2017); *see also MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930, 938-40 (2005) (technology distributor contributorily and vicariously liable for others' unlawful use of technology where the technology has an "unlawful objective"); *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1022-24 (Fed. Cir. 2015) (software designer liable for infringing conduct of its software where designer "condition[ed]" use of software on infringing behavior); *Shaw v. Toshiba Am. Info. Sys.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999) (software designer liable for harm to third-party caused by software).

visited August 4, 2021); William Gallagher, *Wipe Your iPhone Before Selling It, Because If You Don't You Might Get Your Data Stolen*, Apple Insider (Jul 26, 2018), https://appleinsider.com/articles/18/07/26/wipe-your-iphone-before-selling-it-because-if-you-dont-you-might-get-your-data-stolen.

55. Samsung is also vicariously liable under principles of agency law for BIPA violations caused by the use of Samsung Devices because Samsung's Samsung Devices functioned as software agents subject to the actual authority of Samsung, *see* Restatement (Third) of Agency § 7.04 (2006), because Samsung acted negligently in controlling its proprietary software installed on Apple Devices, *see id.* § 7.05, or both.

56. Further, Samsung is vicariously liable because the use of its Samsung Devices was conditioned on unlawful use and had an objective that was unlawful under Illinois law.

VII. Plaintiff's Experience with Samsung's Products.

57. Plaintiff G.T. is an eleven-year-old minor. She owns a Samsung Galaxy A20, which she has used to take photos of herself and other people.

58. G.T. also appears in photographs on her relatives' Samsung Devices.

59. G.T. has not—and cannot—give consent for Samsung to collect or possess her biometric identifiers and biometric information. Further, G.T.'s parents have not given prior informed written consent for Samsung to collect or possess G.T.'s biometric identifiers and biometric information.

60. Plaintiff was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (*e.g.* scans of face geometry, face templates) not only from Plaintiff, but also from other individuals appearing in photographs on Plaintiff's Samsung Device, including parents, siblings (who are minors), cousins (some of whom are minors), and a grandparent of Plaintiff.

61. The Gallery App on Plaintiff's Samsung Device automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already

saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

62. Samsung's facial recognition technology also collected biometric identifiers and information (*e.g.* scans of face geometry, face templates) from photos of Plaintiff stored in the photo libraries of other peoples' Samsung Devices, including her relatives' Samsung Devices.

63. Upon information and belief, the Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff in the photo library automatically compared the face templates of Plaintiff and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

64. At all times relevant, G.T. was unaware of Samsung's facial recognition "feature" of the Gallery App, though she has "tagged" individuals in photographs that Samsung has organized by facial geometry.

65. Samsung has not informed Plaintiff that Biometrics have been and are being collected from the individuals whose faces appear in photographs stored in her Samsung Device.

66. Moreover, Samsung has not informed Plaintiff that the Gallery App is installed on her device by default and will operate on mobile devices whenever a photograph is added to the photo library.

67. Samsung did not obtain consent from Plaintiff in any form prior to harvesting her Biometrics, let alone the written, informed consent required by BIPA.

68. Samsung never provided Plaintiff with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

69. By collecting Plaintiff's unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded Plaintiff's statutorily protected right to privacy in her Biometrics.

70. Further, Samsung never provided Plaintiff with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

71. Samsung's acts and omissions denied Plaintiff the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and/ biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

CLASS ALLEGATIONS

72. **Class Definition:** Plaintiff brings this action on behalf of a class of all similarly-situated individuals (the "Class") that is defined, subject to amendment, as follows:

> All individuals who, while residing in the State of Illinois, had their biometric identifiers or biometric information collected, captured, received or otherwise obtained and/or stored by Samsung.

73. Plaintiff represents and is a member of the Class. Excluded from the Class are Samsung and any entities in which Samsung has a controlling interest, Samsung's employees and agents, the Judge to whom this action is assigned, and any member of the Judge's staff and immediate family.

74. Certification of Plaintiff's claim for classwide treatment is appropriate because Plaintiff can prove the elements of her claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

75. **Numerosity**. The number of persons within the Class is substantial, and is

reasonably believed to include thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. While the exact number of Class member is currently unknown, this information can be ascertained from Samsung's and third-parties' records. Class members can be notified about the pendency of this action through recognized, Court-approved methods of notice dissemination, such as U.S. Mail, electronic mail, internet postings, and/or published notice.

76. **Commonality and Predominance**. This action involves common questions of law and fact, which predominate over any questions affecting Class members, including, without limitation;

(a) whether Samsung collected or otherwise obtained the Class members' biometric identifiers or biometric information;

(b) whether Samsung possessed the Class members' biometric identifiers or biometric information;

(c) whether Samsung informed the Class members in writing that their biometric identifiers and biometric information are being collected or stored;

(d) whether Samsung informed Class members in writing of the specific purposes and length of term for which their biometric identifiers and biometric information are being collected, stored, and used;

(e) whether Samsung received a signed written release (as defined in 740 ILCS 14/10) to collect, use, and store the Class members' biometric identifiers and biometric information;

(f) whether Samsung maintained a publicly-available written policy establishing a retention schedule and guidelines for the destruction of biometric identifiers and information at the time it collected the Class members' biometric identifiers and biometric information;

(g) whether Samsung complied with any such written policy;

(h) whether Samsung permanently destroyed the Class members' biometric identifiers and biometric information;

(i) whether Samsung used the Class members' biometric identifiers or biometric information to identify them;

(j) whether Samsung violated BIPA; and

(k) whether Samsung's violations of BIPA were negligent, reckless, or intentional.

77. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex and class action litigation. Plaintiff has no interests antagonistic to those of the Class.

78. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiff and the Class)

79. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

80. BIPA requires private entities in possession of Biometrics to establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those entities must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent destruction of biometric data (at most three years after the entity's last interaction with the individual); and (ii) adhere to that retention schedule and actually delete the biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

81. Samsung failed to comply with either of these BIPA mandates.

82. Samsung is a company registered to do business in Illinois, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

83. Plaintiff and the Class members are individuals whose biometric identifiers and/or biometric information are possessed by Samsung.

84. In violation of BIPA, Samsung did not maintain the statutorily-mandated retention schedule and destruction guidelines at the time it collected Plaintiff's and the Class member's biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

85. In violation of BIPA, Samsung did not permanently destroy Plaintiff's and the Class members' biometric identifiers and biometric information as required. *See* 740 ILCS 14/15(a).

86. By failing to destroy Plaintiff's and the Class members' biometric identifiers and biometric information, Samsung unlawfully retained their Biometrics.

87. Samsung's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

88. In the alternative, Samsung's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

89. Accordingly, Plaintiff, on behalf of herself and the Class, seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Samsung to immediately and permanently destroy their biometric identifiers and biometric information, and to comply with BIPA's requirements that private entities maintain and comply with publicly-available guidelines for permanently destroying biometric identifiers and biometric information; (3) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorney's fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiff and the Class)

90. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

91. BIPA requires private entities such as Samsung to obtain informed written consent from individuals before acquiring their Biometrics. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's . . . biometric identifier or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric

identifier or biometric information is being collected, stored, and used; **and** (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .” 740 ILCS 14/15(b).

92. Samsung is a company registered to do business in Illinois, and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

93. Plaintiff and the Class members are individuals whose “biometric identifiers” and “biometric information,” as defined by the BIPA—including, without limitation, scans of their facial geometry—were collected or otherwise obtained, stored, and used by Samsung.

94. Samsung violated BIPA by failing to inform Plaintiff and the Class, in writing, about the collection and storage of their biometric identifiers and biometric information before it occurred. *See* 740 ILCS 14/15(b)(1).

95. Samsung violated BIPA by failing to inform Plaintiff and the Class, in writing before the fact, of the specific purpose and length of term for which their biometric identifiers and biometric information were being “collected, stored, and used” before it occurred. *See* 740 ILCS 14/15(b)(2).

96. Samsung violated BIPA by collecting, capturing, purchasing, receiving through trade, and otherwise obtaining Plaintiff’s and the Class members’ biometric identifiers and biometric information without first obtaining a signed written release from each of them. *See* 740 ILCS 14/15(b)(3).

97. In so doing, Samsung deprived Plaintiff and the Class of their statutory right to maintain the privacy of their biometric identifiers and biometric information.

98. Samsung’s conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

99. In the alternative, Samsung's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

100. Accordingly, Plaintiff, on behalf of herself and the Class, seeks: (1) declaratory relief; (2) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); (3) injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Samsung to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, as described herein; and (4) reasonable attorney's fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff G.T., by and through next friend Liliana T. Hanlon, on behalf of herself and the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above (or on behalf of any other class the Court deems appropriate);

B. Appointing Plaintiff as representative of the Class, and her undersigned attorneys as class counsel;

C. Declaring that Samsung's acts and omissions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

D. Awarding statutory damages of $5,000 for each and every intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 for each and every negligent violation pursuant to 740 ILCS 14/20(1) if the Court finds that Samsung's violations were negligent;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including, *inter alia*, requiring Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, and to permanently destroy Plaintiff's and the Class members' biometric identifiers and biometric information;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiff and the Class members pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff, individually and on behalf of all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: October 8, 2021

Respectfully submitted,

G.T., BY AND THROUGH NEXT FRIEND LILIANA T. HANLON, individually and on behalf of all others similarly situated, Plaintiff

By: /s/ Keith J. Keogh

Keith J. Keogh
Theodore H. Kuyper
Gregg M. Barbakoff
KEOGH LAW, LTD.
55 W. Monroe Street, Suite 3390
Chicago, Illinois 60603
(312) 726-1092
keith@keoghlaw.com
tkuyper@keoghlaw.com
gbarbakoff@keoghlaw.com

Attorneys for Plaintiff and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that, on October 8, 2021, I caused a copy of the foregoing ***Amended Class Action Complaint*** to be served upon all counsel of record via electronic filing using the CM/ECF system.

/s/ Keith J. Keogh